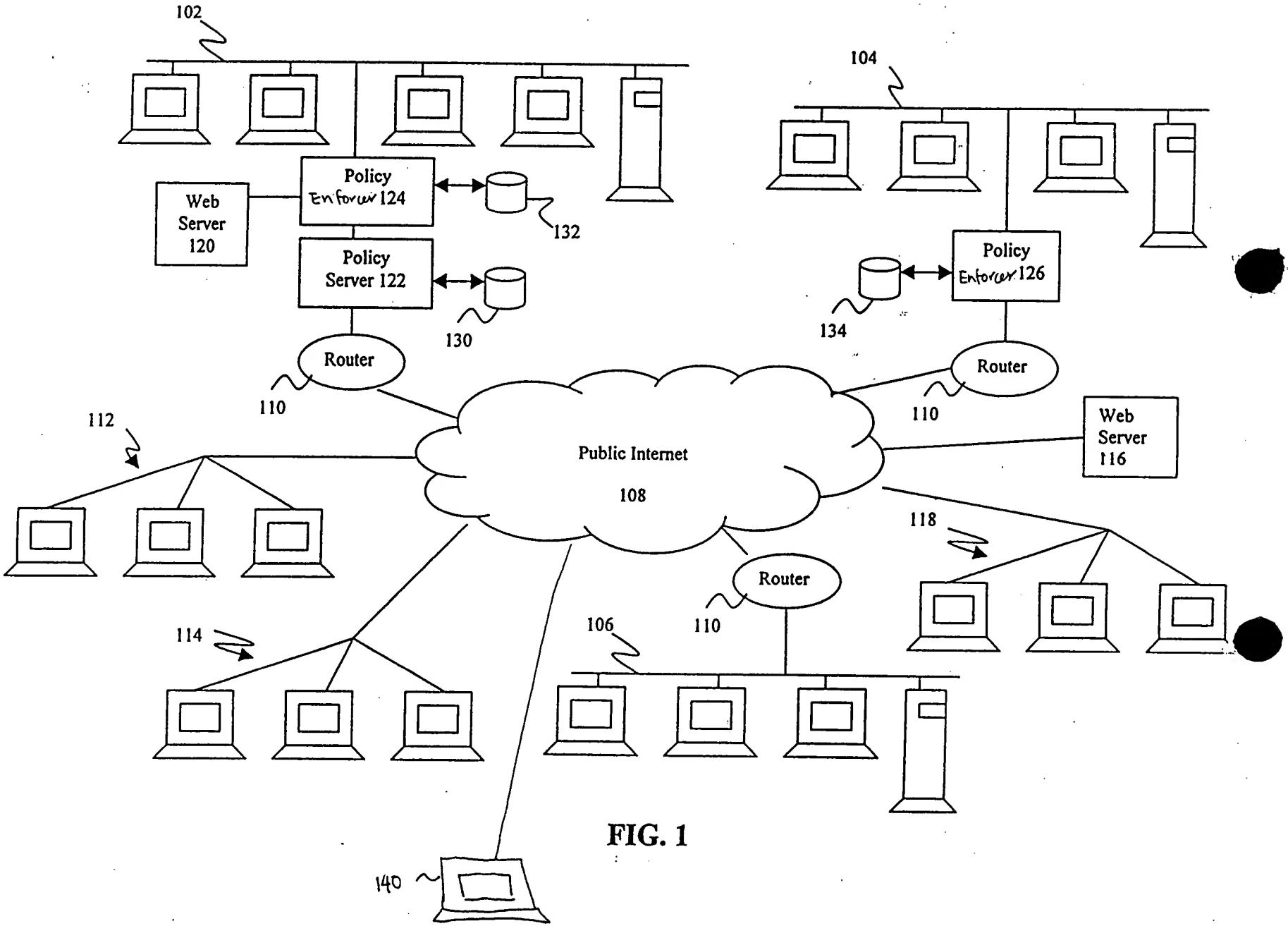

102
104
Policy Enforcer 124
Web Server 120
132
Policy Server 122
130
Policy Enforcer 126
134
Router
110
Router
110
112
Public Internet
108
Web Server 116
118
Router
110
106
114
140

FIG. 1

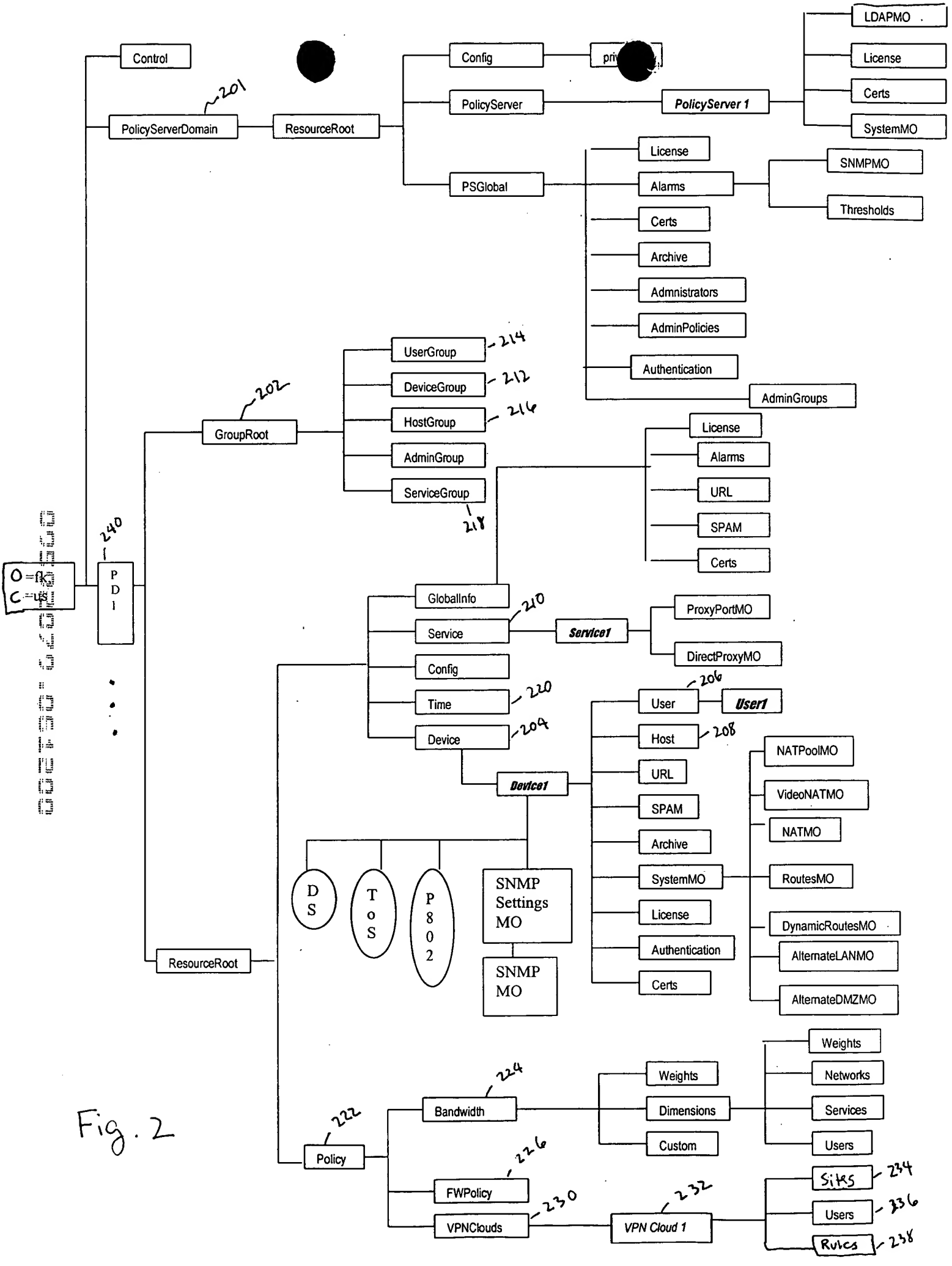

Control
PolicyServerDomain
201
ResourceRoot
Config
PolicyServer
PSGlobal
PolicyServer 1
LDAPMO
License
Certs
SystemMO
License
Alarms
SNMPMO
Thresholds
Certs
Archive
Admnistrators
AdminPolicies
Authentication
AdminGroups
GroupRoot
202
UserGroup
214
DeviceGroup
212
HostGroup
216
AdminGroup
ServiceGroup
218
License
Alarms
URL
SPAM
Certs
240
PDI
GlobalInfo
Service
210
Service1
ProxyPortMO
DirectProxyMO
Config
Time
220
Device
204
Device1
User
206
User1
Host
208
URL
SPAM
Archive
SystemMO
License
Authentication
Certs
NATPoolMO
VideoNATMO
NATMO
RoutesMO
DynamicRoutesMO
AlternateLANMO
AlternateDMZMO
DS
ToS
P802
SNMP Settings MO
SNMP MO
ResourceRoot
Policy
222
Bandwidth
224
FWPolicy
226
VPNClouds
230
Weights
Dimensions
Custom
Weights
Networks
Services
Users
VPN Cloud 1
232
Sites
234
Users
236
Rules
238

Fig. 2

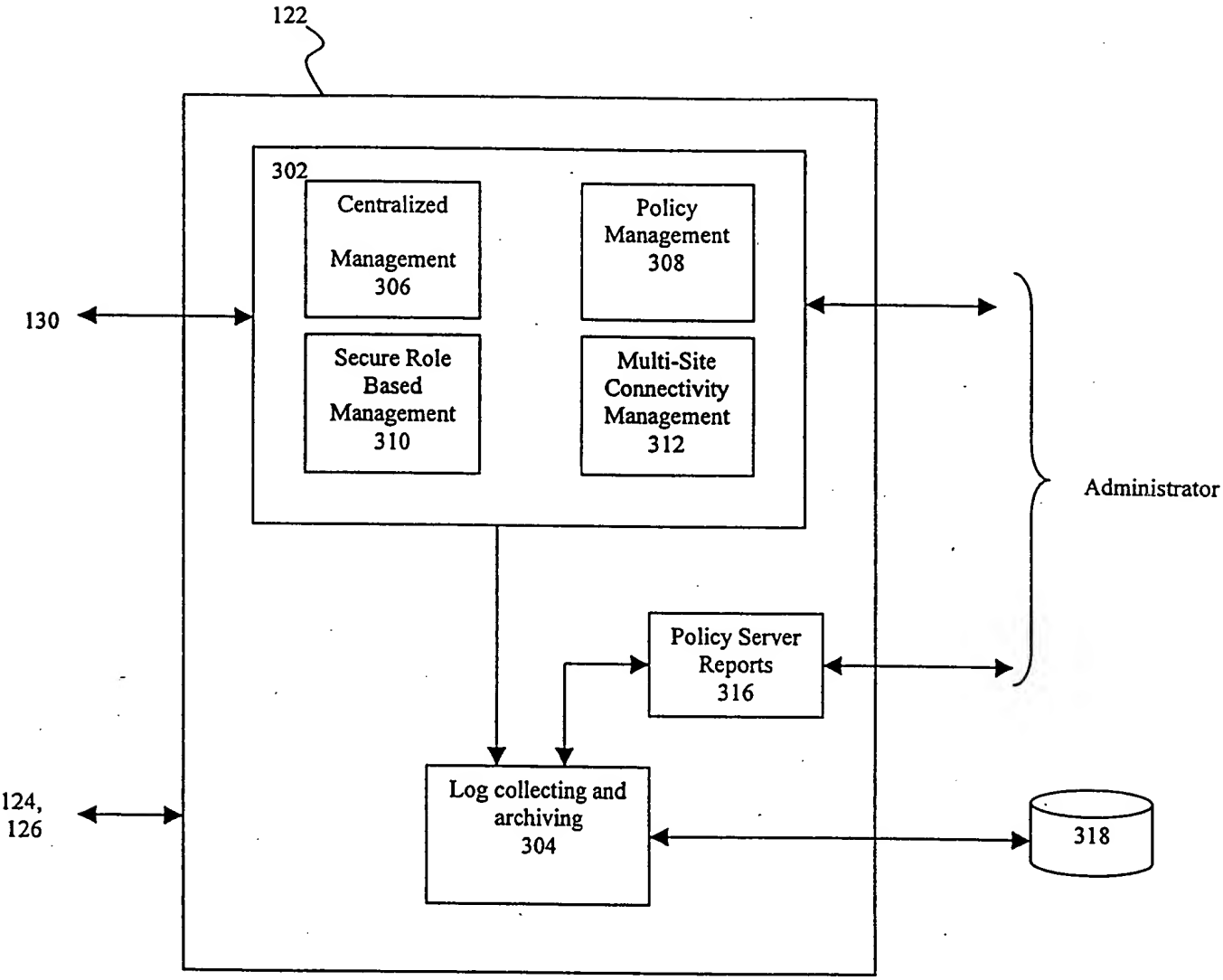

122
302
Centralized Management 306
Policy Management 308
Secure Role Based Management 310
Multi-Site Connectivity Management 312
130
Administrator
Policy Server Reports 316
Log collecting and archiving 304
124, 126
318

FIG. 3

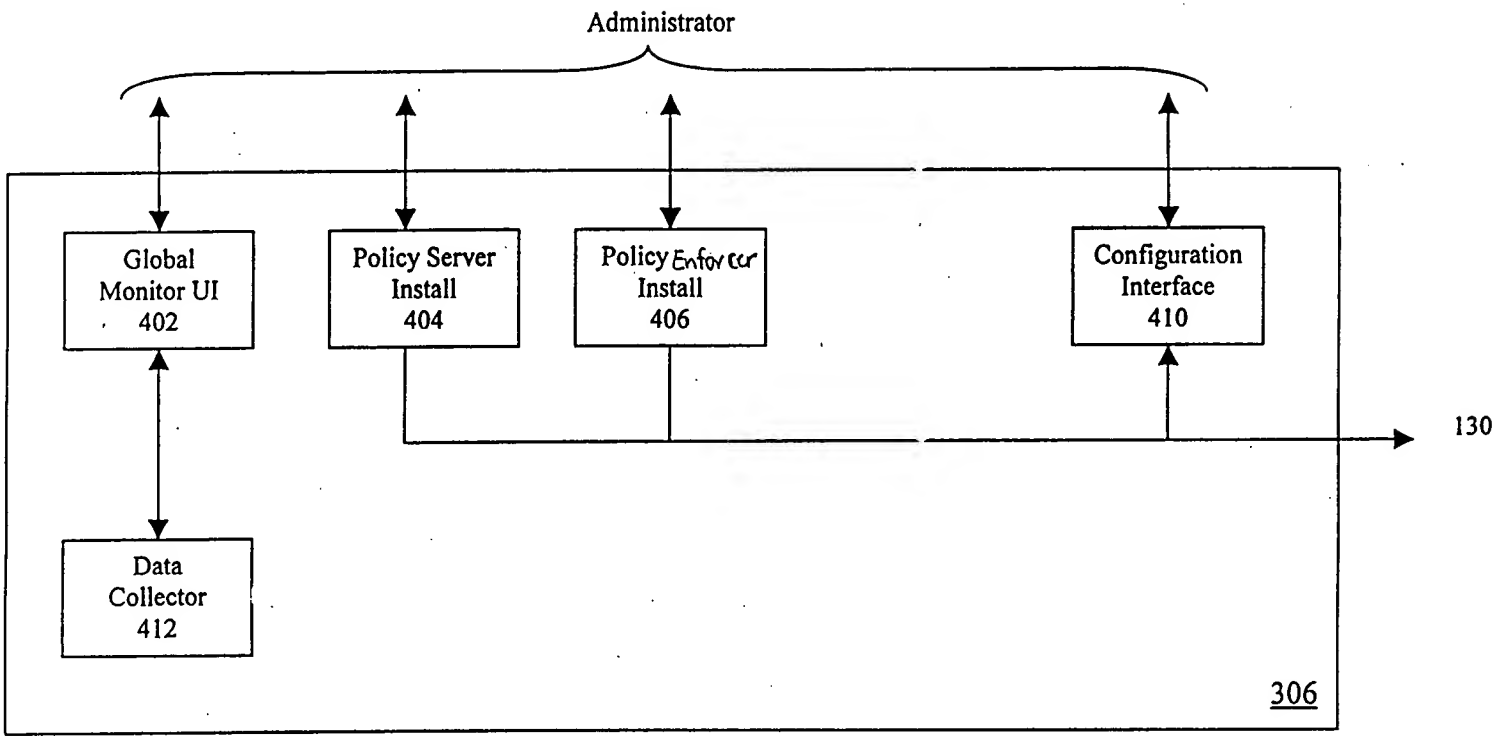

Administrator
Global Monitor UI 402
Policy Server Install 404
Policy Enforcer Install 406
Configuration Interface 410
Data Collector 412
130
306

FIG. 4

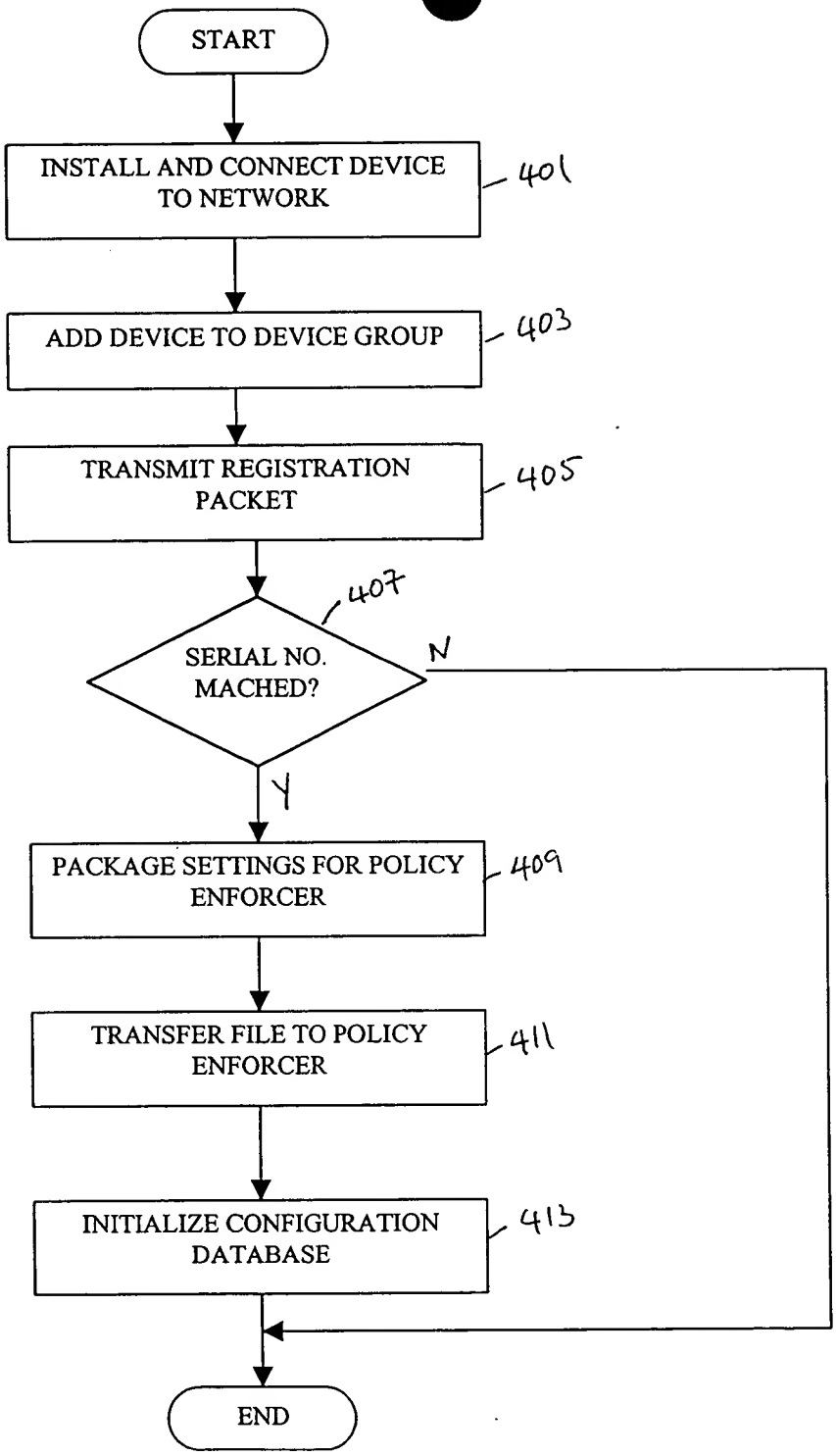

START
INSTALL AND CONNECT DEVICE TO NETWORK
401
ADD DEVICE TO DEVICE GROUP
403
TRANSMIT REGISTRATION PACKET
405
407
SERIAL NO. MACHED?
N
Y
PACKAGE SETTINGS FOR POLICY ENFORCER
409
TRANSFER FILE TO POLICY ENFORCER
411
INITIALIZE CONFIGURATION DATABASE
413
END

FIG. 5

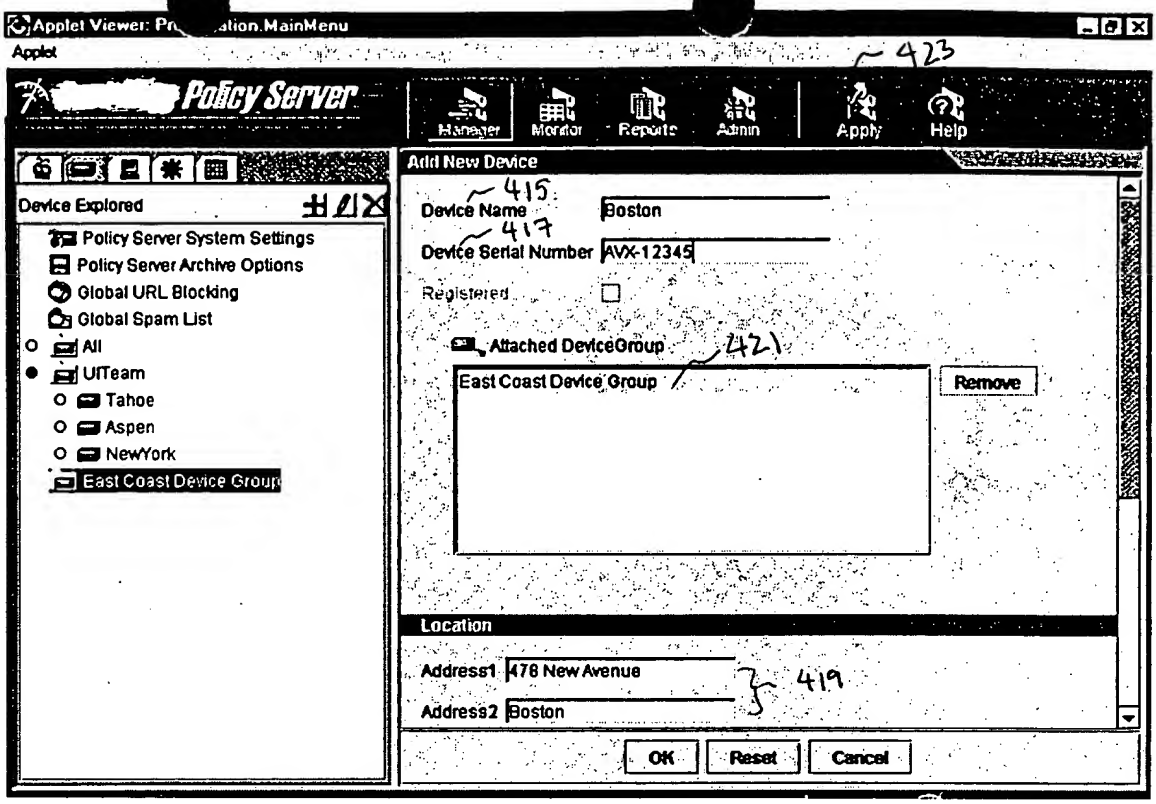

Applet Viewer: Pr ation.MainMenu
Applet
~423
Policy Server
Manager
Monitor
Reports
Admin
Apply
Help
Device Explored
Policy Server System Settings
Policy Server Archive Options
Global URL Blocking
Global Spam List
All
UITeam
Tahoe
Aspen
NewYork
East Coast Device Group
Add New Device
~415
Device Name
Boston
~417
Device Serial Number
AVX-12345
Registered
Attached DeviceGroup
421
East Coast Device Group
Remove
Location
Address1
478 New Avenue
419
Address2
Boston
OK
Reset
Cancel

Fig. 6

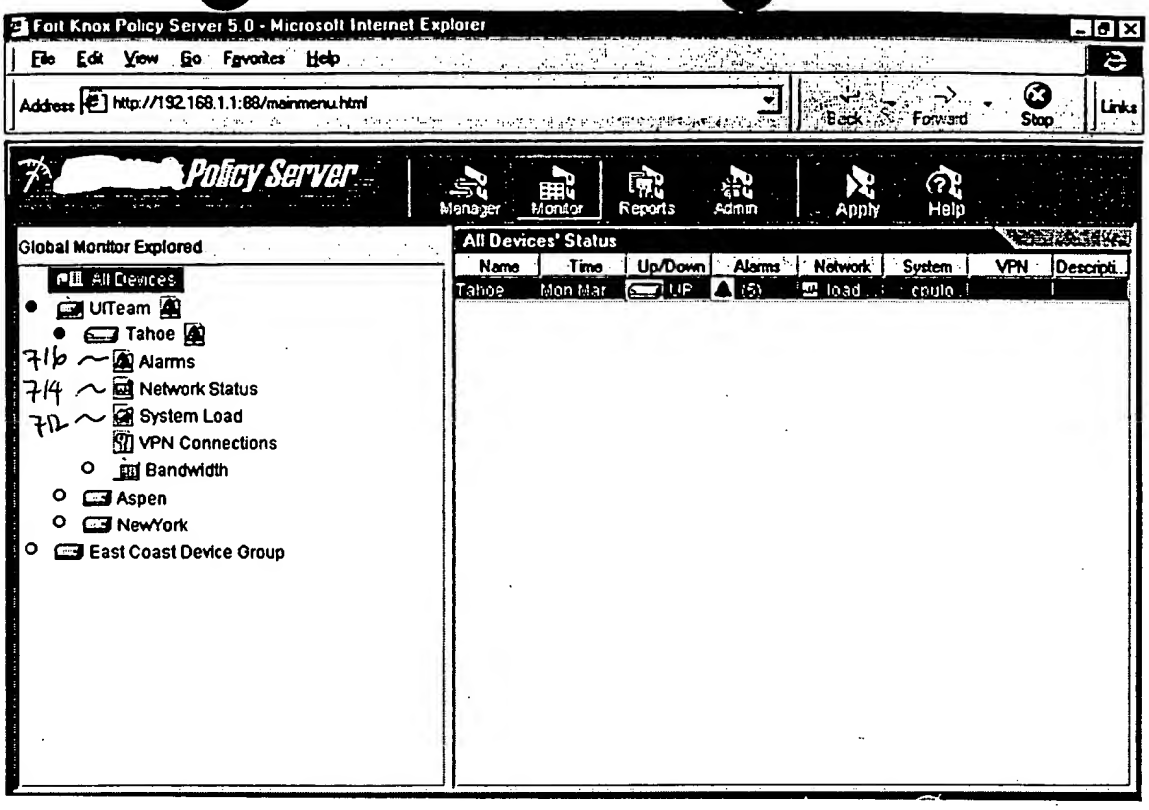

Fort Knox Policy Server 5.0 - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://192.168.1.1:88/mainmenu.html
Back Forward Stop Links
Policy Server
Manager Monitor Reports Admin Apply Help
Global Monitor Explored
All Devices
UITeam
Tahoe
716 Alarms
714 Network Status
712 System Load
VPN Connections
Bandwidth
Aspen
NewYork
East Coast Device Group
All Devices' Status
Name Time Up/Down Alarms Network System VPN Descripti
Tahoe Mon Mar UP load

Fig. 7

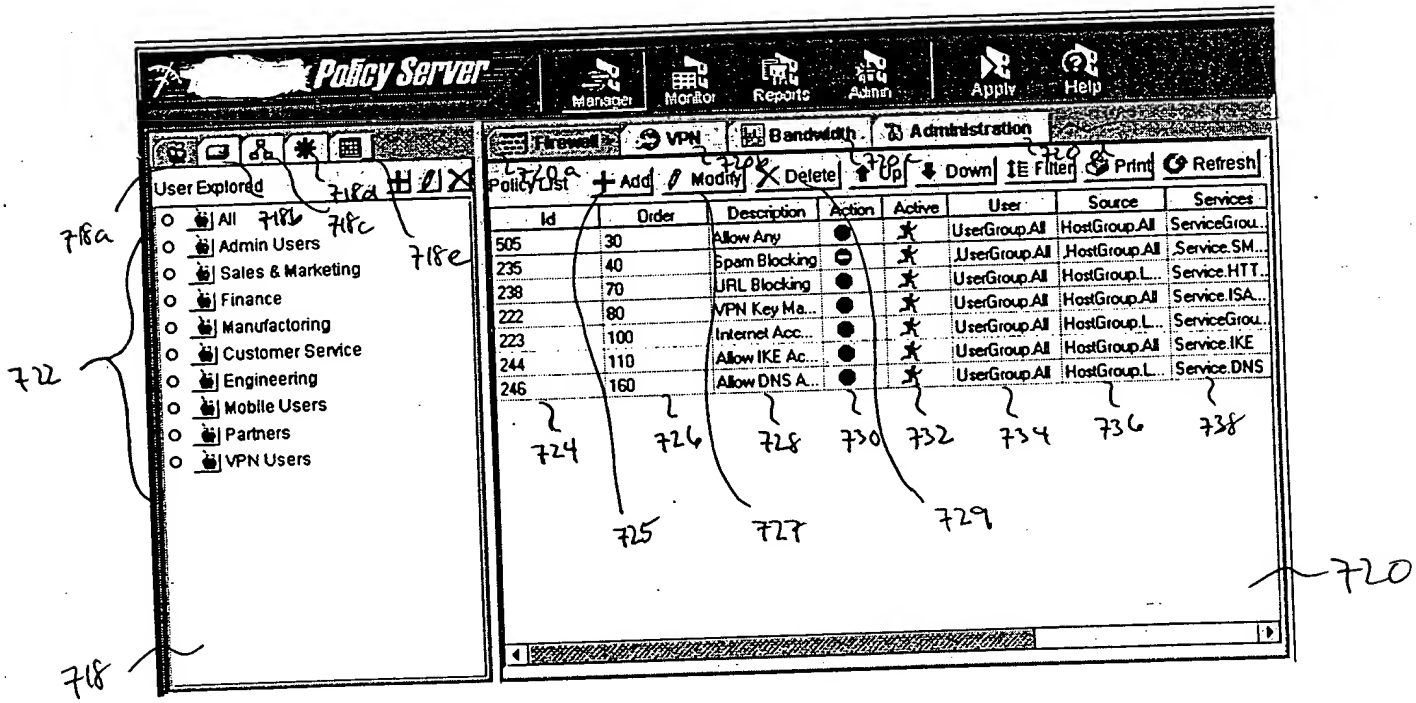

Policy Server
Manage
Monitor
Reports
Admin
Apply
Help
Firewall
VPN
Bandwidth
Administration
User Explored
All
Admin Users
Sales & Marketing
Finance
Manufactoring
Customer Service
Engineering
Mobile Users
Partners
VPN Users
Policy List
Add
Modify
Delete
Up
Down
Filter
Print
Refresh
Id
Order
Description
Action
Active
User
Source
Services
505
30
Allow Any
UserGroup.All
HostGroup.All
ServiceGrou...
235
40
Spam Blocking
UserGroup.All
HostGroup.All
Service.SM...
238
70
URL Blocking
UserGroup.All
HostGroup.L...
Service.HTT...
222
80
VPN Key Ma...
UserGroup.All
HostGroup.All
Service.ISA...
223
100
Internet Acc...
UserGroup.All
HostGroup.L...
ServiceGrou...
244
110
Allow IKE Ac...
UserGroup.All
HostGroup.All
Service.IKE
246
160
Allow DNS A...
UserGroup.All
HostGroup.L...
Service.DNS
718a
718b
718c
718d
718e
722
718
720
720a
720b
720c
720d
720e
724
725
726
727
728
729
730
732
734
736
738

Fig. 8

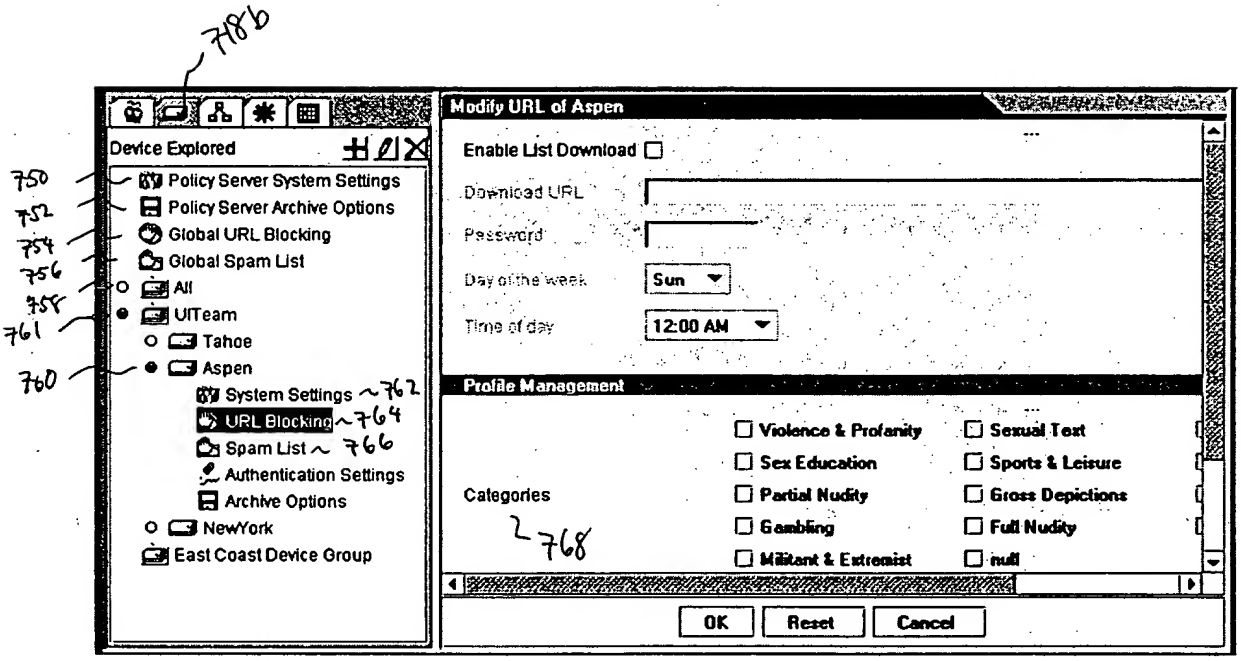

786
Device Explored
Policy Server System Settings
Policy Server Archive Options
Global URL Blocking
Global Spam List
All
UITeam
Tahoe
Aspen
System Settings
URL Blocking
Spam List
Authentication Settings
Archive Options
NewYork
East Coast Device Group
750
752
754
756
758
761
760
762
764
766
Modify URL of Aspen
Enable List Download
Download URL
Password
Day of the week
Sun
Time of day
12:00 AM
Profile Management
Categories
768
Violence & Profanity
Sex Education
Partial Nudity
Gambling
Militant & Extremist
Sexual Text
Sports & Leisure
Gross Depictions
Full Nudity
null
OK
Reset
Cancel

Fig. 9

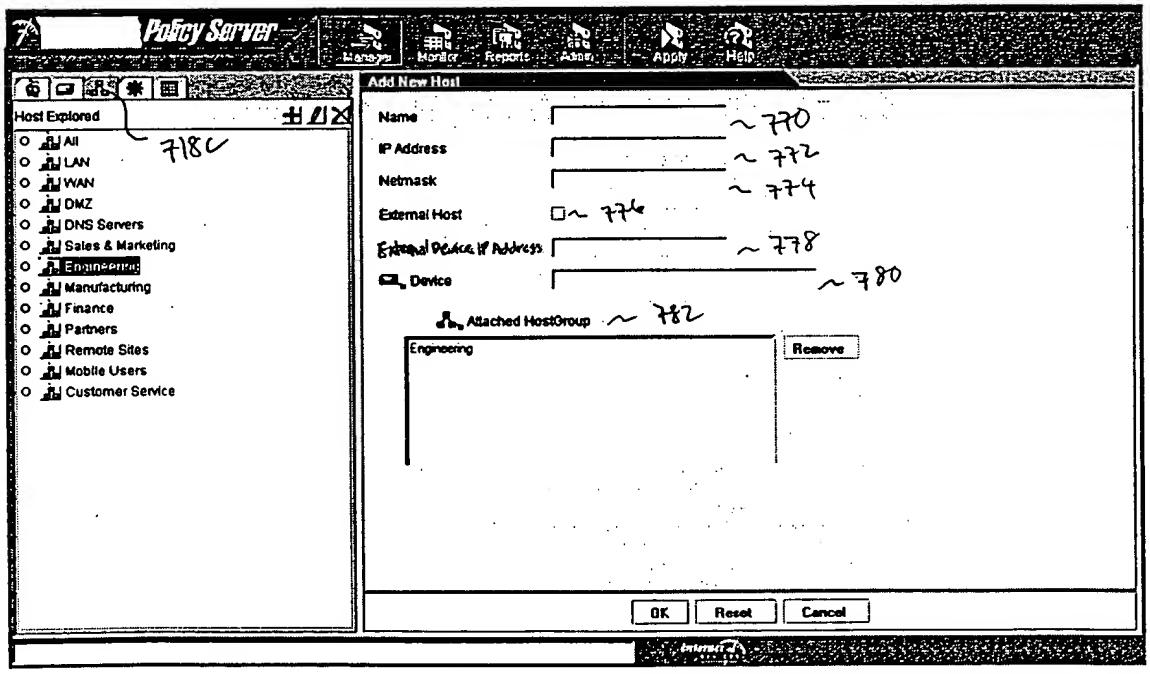

Policy Server
Manage
Monitor
Reports
Admin
Apply
Help
Host Explored
All
LAN
WAN
DMZ
DNS Servers
Sales & Marketing
Engineering
Manufacturing
Finance
Partners
Remote Sites
Mobile Users
Customer Service
718C
Add New Host
Name
IP Address
Netmask
External Host
External Device IP Address
Device
Attached HostGroup
Engineering
Remove
OK
Reset
Cancel
770
772
774
776
778
780
782

Fig. 10

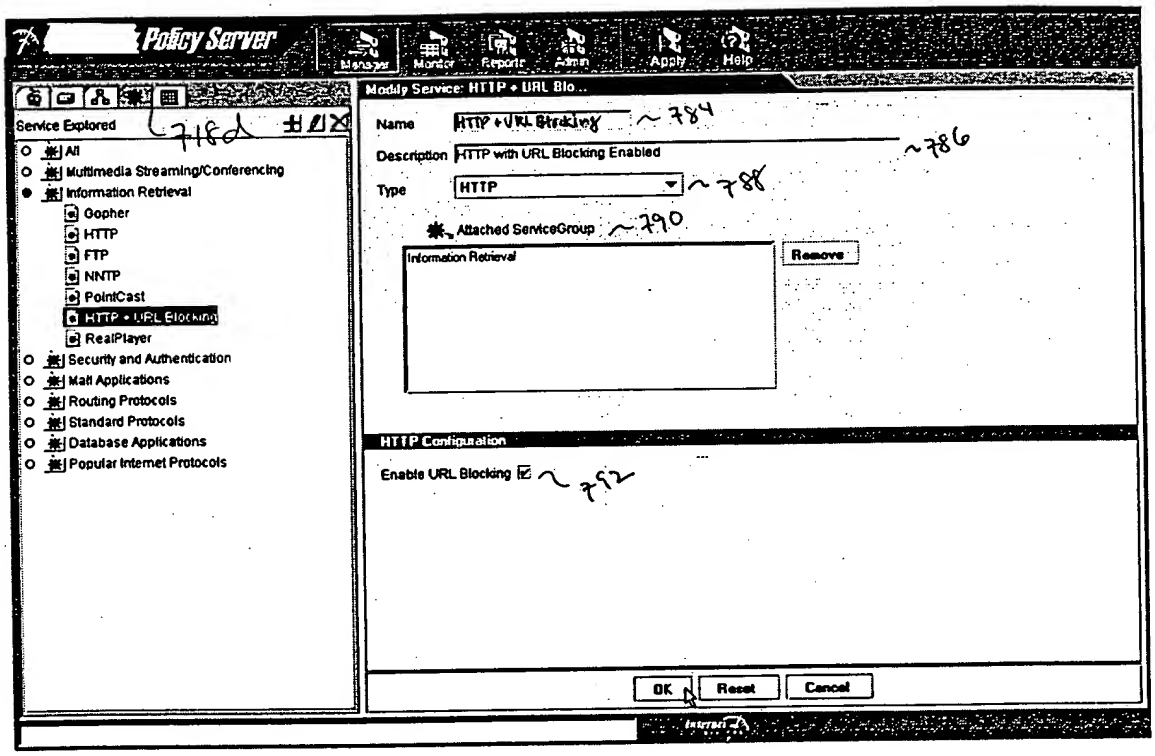

Policy Server
Manager
Monitor
Reports
Admin
Apply
Help
Service Explored
718d
All
Multimedia Streaming/Conferencing
Information Retrieval
Gopher
HTTP
FTP
NNTP
PointCast
HTTP + URL Blocking
RealPlayer
Security and Authentication
Mail Applications
Routing Protocols
Standard Protocols
Database Applications
Popular Internet Protocols
Modify Service: HTTP + URL Blo...
Name
HTTP + URL Blocking
784
Description
HTTP with URL Blocking Enabled
786
Type
HTTP
788
Attached ServiceGroup
790
Information Retrieval
Remove
HTTP Configuration
Enable URL Blocking
792
OK
Reset
Cancel

Fig. 11

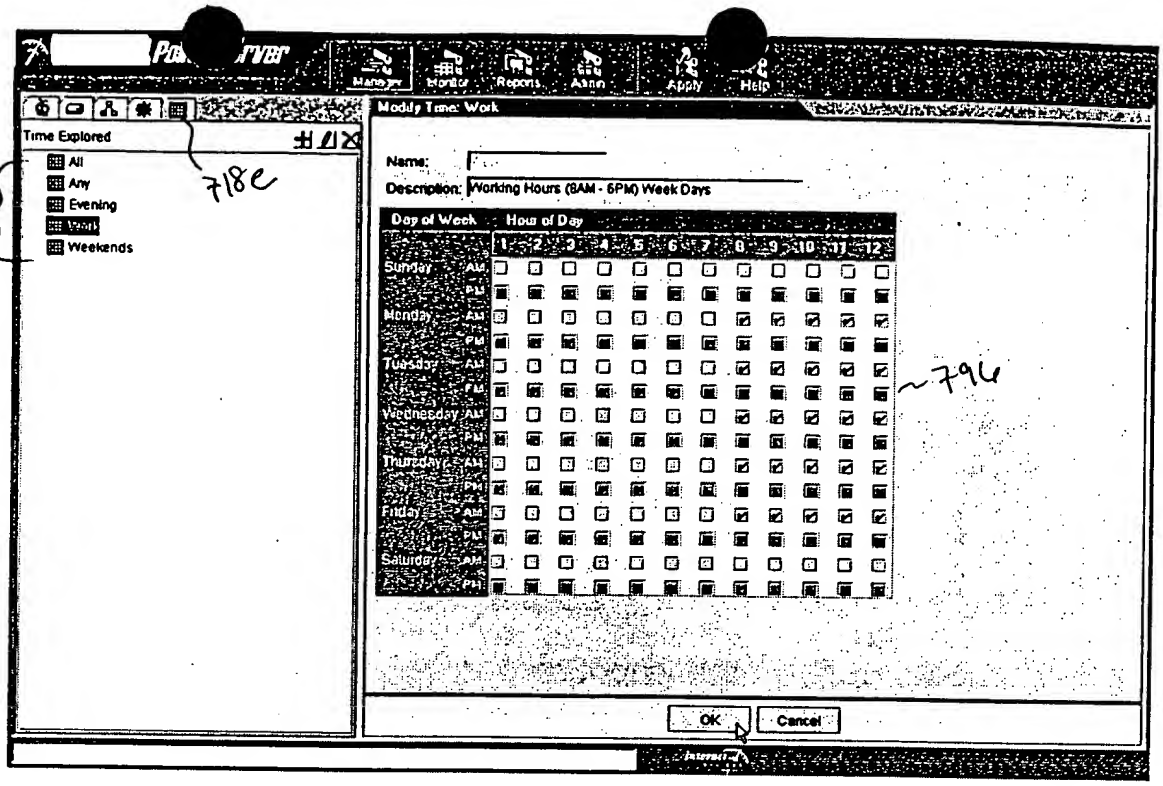

Manage
Monitor
Reports
Admin
Apply
Help
Time Explored
All
Any
Evening
Work
Weekends
718c
794
Modify Time: Work
Name:
Description: Working Hours (8AM - 6PM) Week Days
Day of Week
Hour of Day
1 2 3 4 5 6 7 8 9 10 11 12
Sunday AM
PM
Monday AM
PM
Tuesday AM
PM
Wednesday AM
PM
Thursday AM
PM
Friday AM
PM
Saturday AM
PM
796
OK
Cancel

Fig. 12

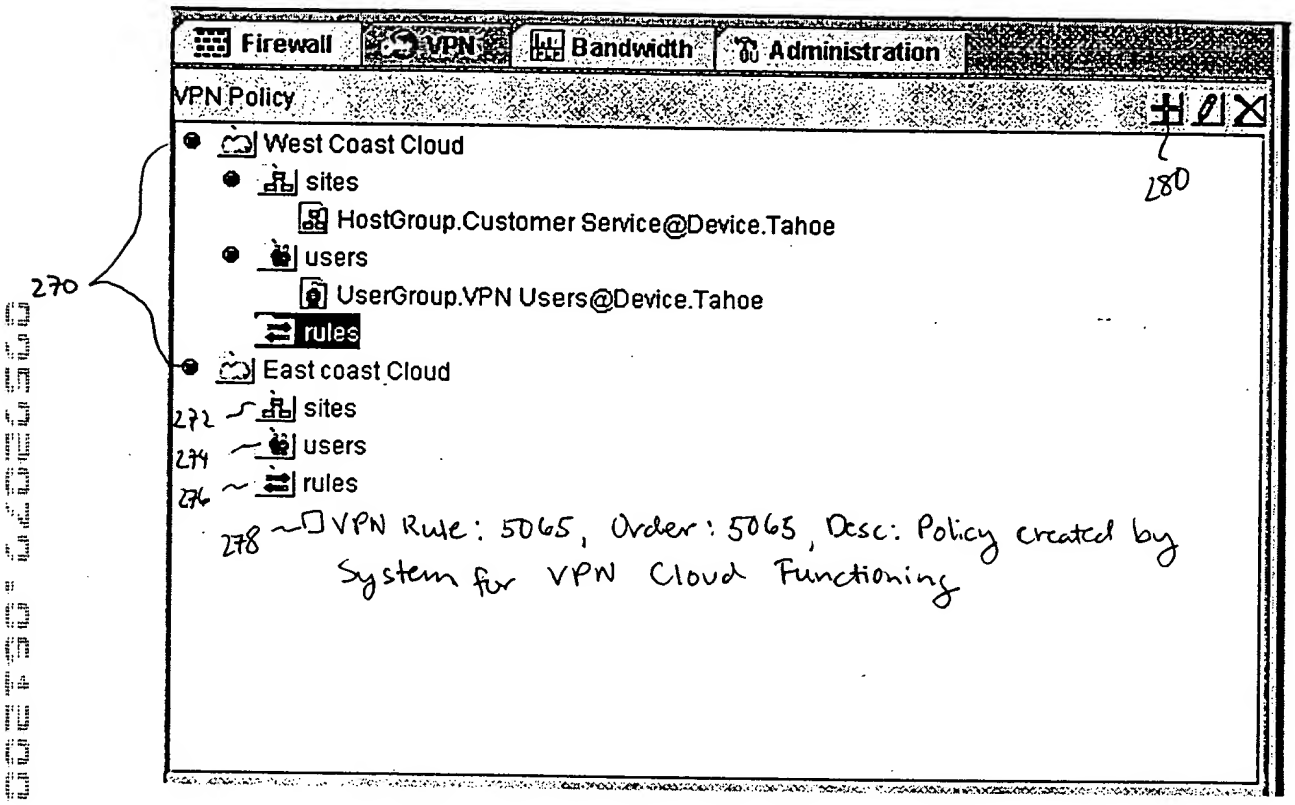

Firewall
VPN
Bandwidth
Administration
VPN Policy
West Coast Cloud
sites
HostGroup.Customer Service@Device.Tahoe
users
UserGroup.VPN Users@Device.Tahoe
rules
East coast Cloud
sites
users
rules
VPN Rule: 5065, Order: 5065, Desc: Policy created by System for VPN Cloud Functioning
270
272
274
276
278
280

FIG. 13

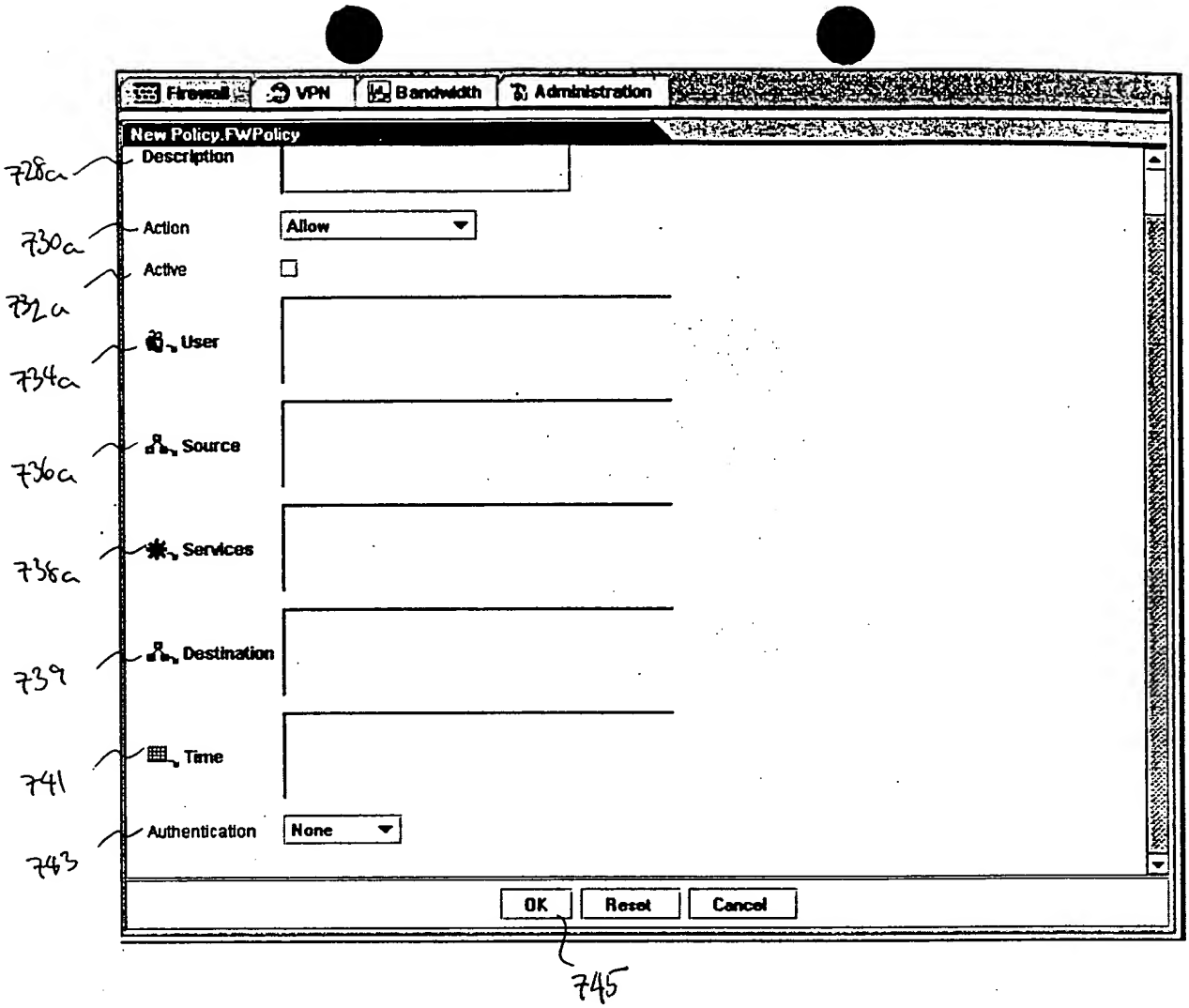

Firewall
VPN
Bandwidth
Administration
New Policy.FWPolicy
Description
Action
Allow
Active
User
Source
Services
Destination
Time
Authentication
None
OK
Reset
Cancel
728a
730a
732a
734a
736a
738a
739
741
743
745

Fig. 14

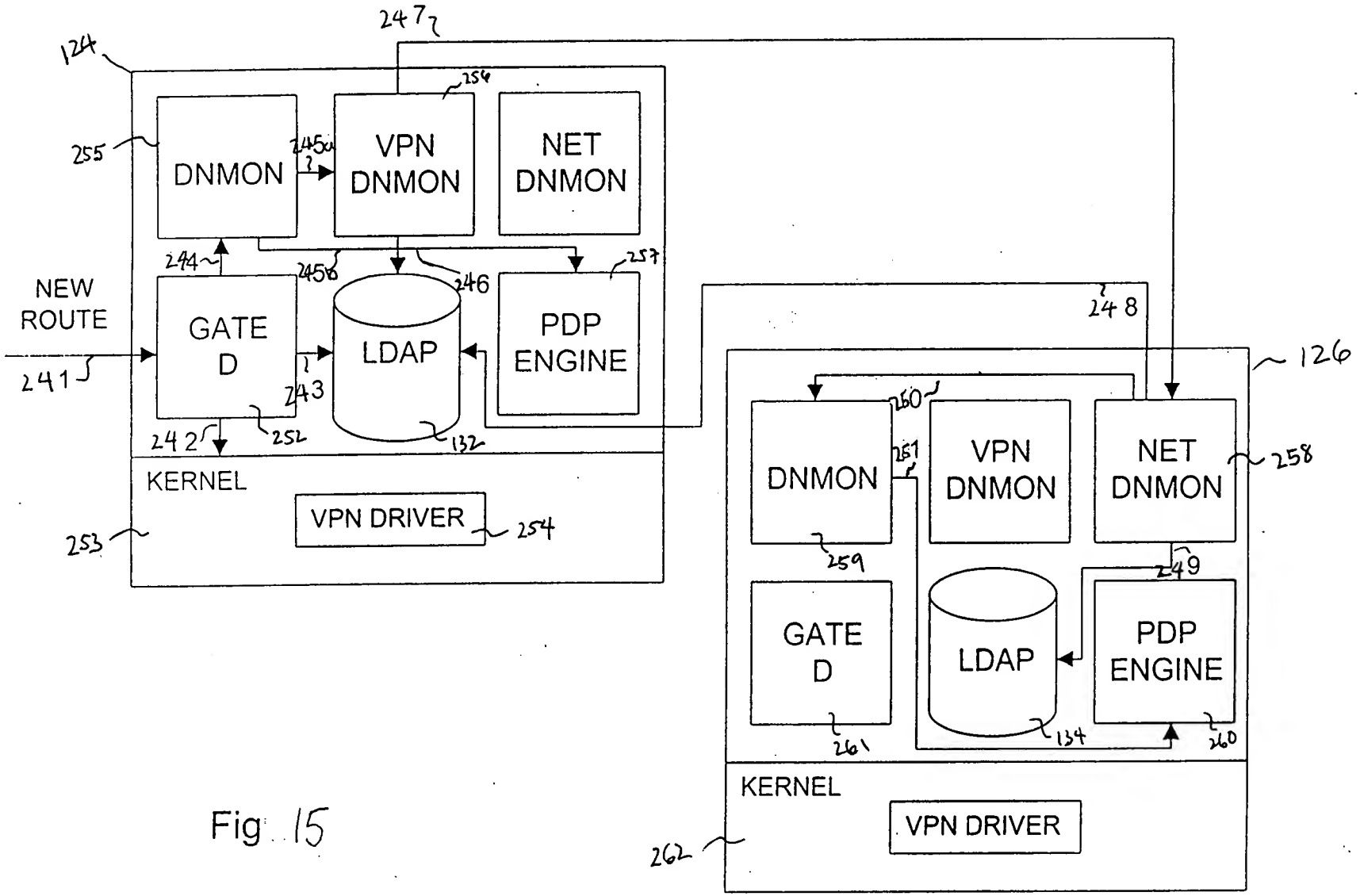

124
247
254
255
DNMON
245a
VPN DNMON
NET DNMON
244
245b
246
257
NEW ROUTE
GATE D
LDAP
PDP ENGINE
241
243
242
252
132
KERNEL
253
VPN DRIVER
254
248
126
260
DNMON
261
VPN DNMON
NET DNMON
258
259
249
GATE D
LDAP
PDP ENGINE
261
134
260
KERNEL
VPN DRIVER
262

Fig. 15

FIG. 16

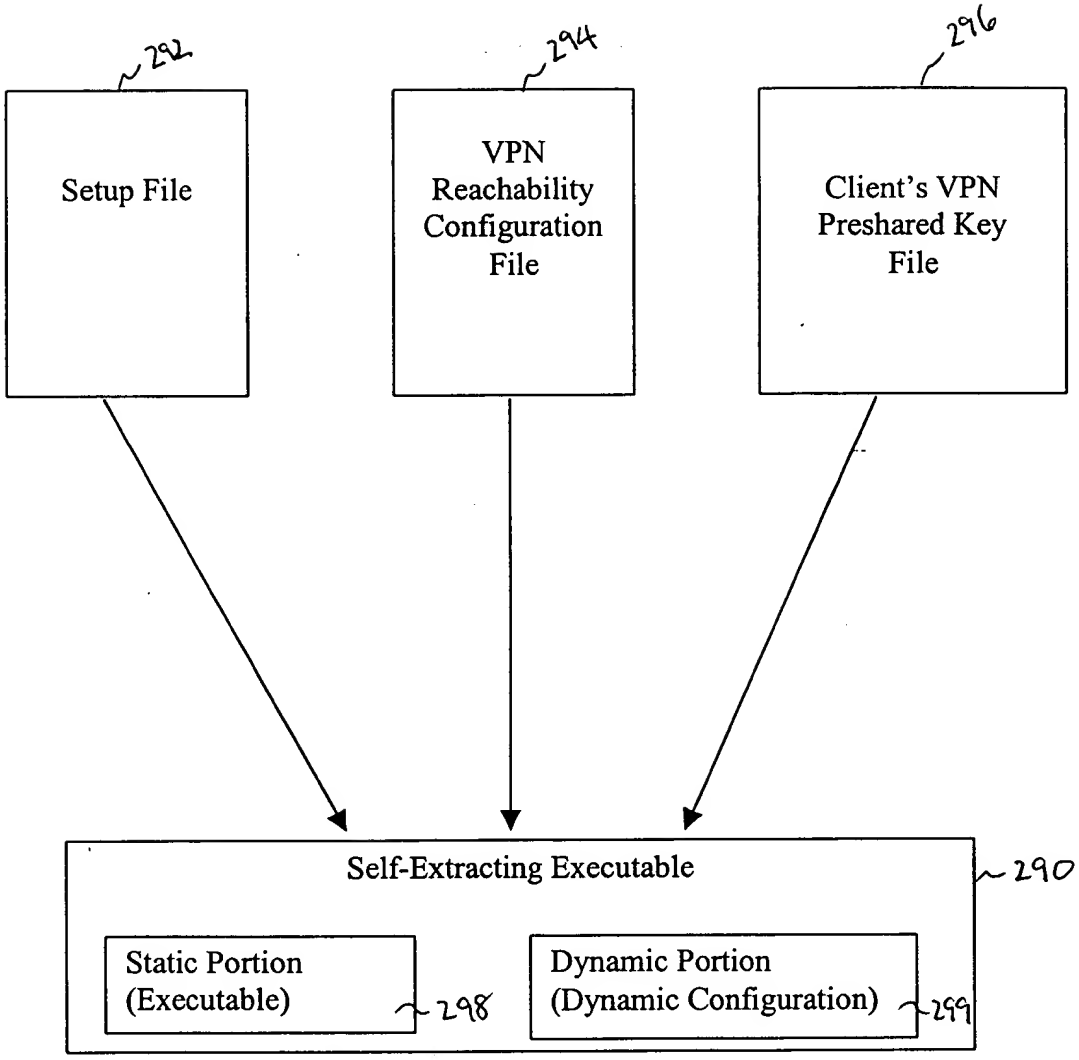
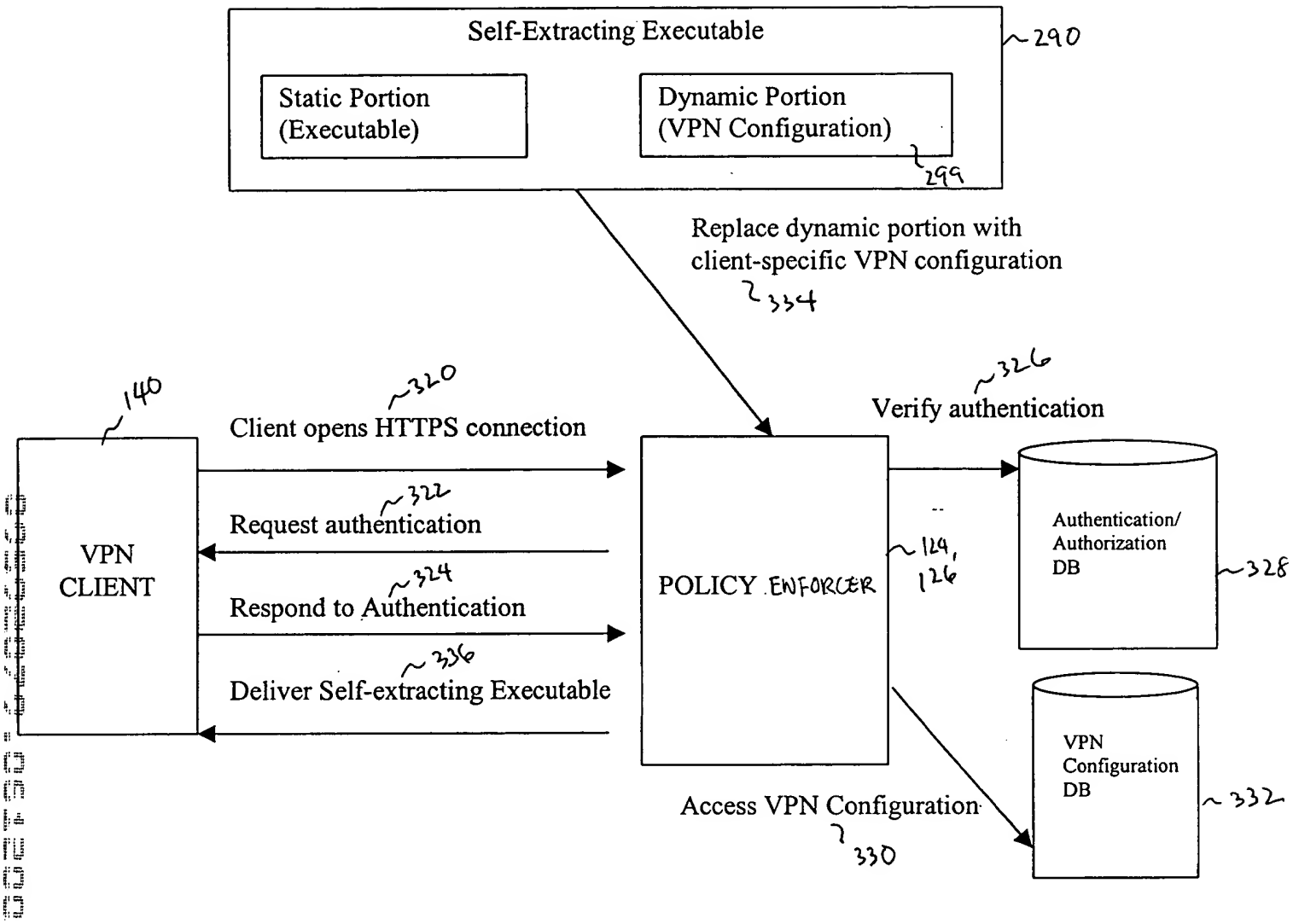

292
294
296
Setup File
VPN Reachability Configuration File
Client's VPN Preshared Key File
Self-Extracting Executable
290
Static Portion (Executable)
298
Dynamic Portion (Dynamic Configuration)
299

FIG. 17


Self-Extracting Executable
290
Static Portion (Executable)
Dynamic Portion (VPN Configuration)
299
Replace dynamic portion with client-specific VPN configuration
334
140
320
Client opens HTTPS connection
326
Verify authentication
VPN CLIENT
322
Request authentication
324
Respond to Authentication
336
Deliver Self-extracting Executable
POLICY ENFORCER
124, 126
Authentication/ Authorization DB
328
VPN Configuration DB
332
Access VPN Configuration
330

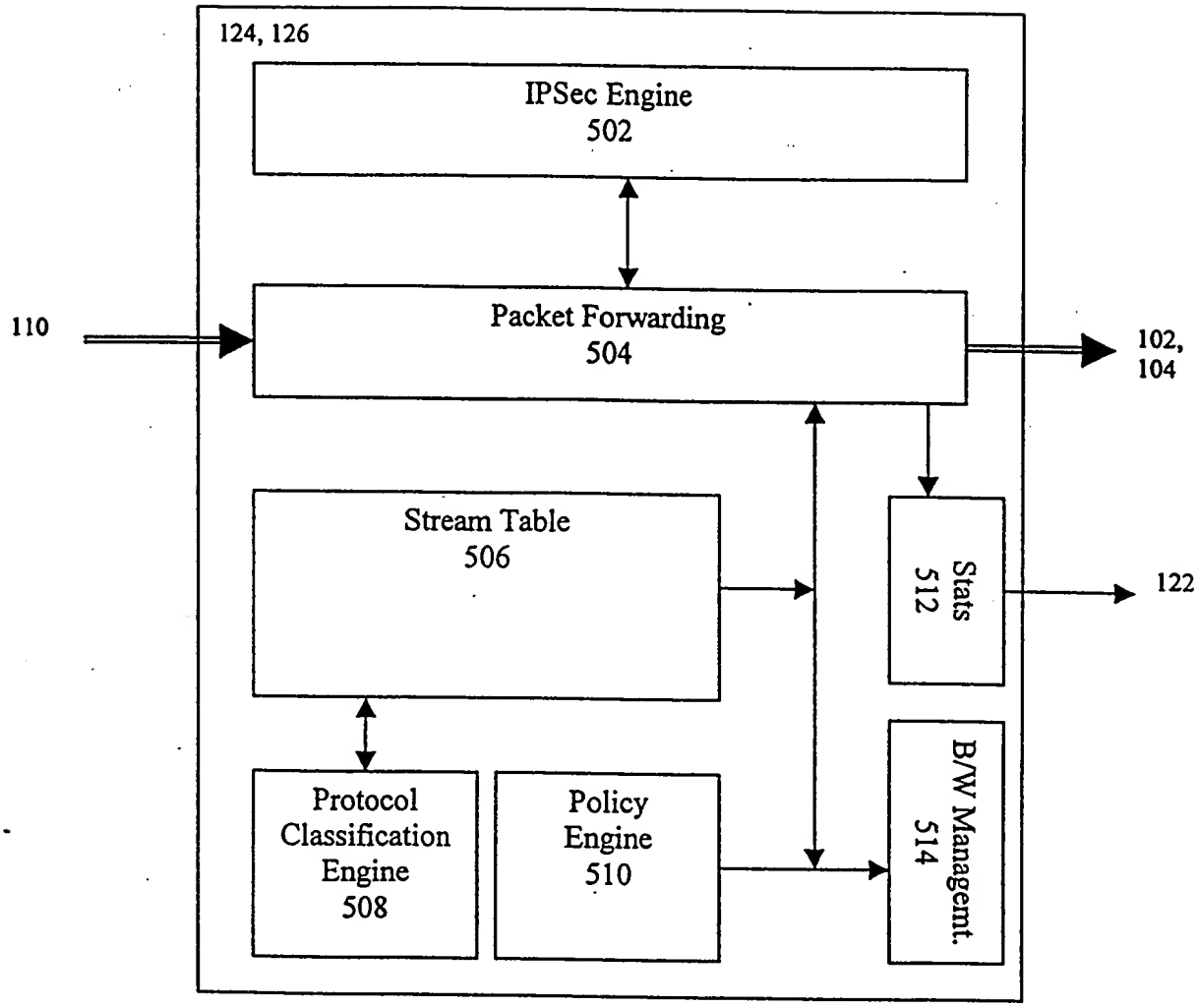

124, 126
IPSec Engine
502
110
Packet Forwarding
504
102,
104
Stream Table
506
Stats
512
122
Protocol
Classification
Engine
508
Policy
Engine
510
B/W Managemt.
514

FIG. 18

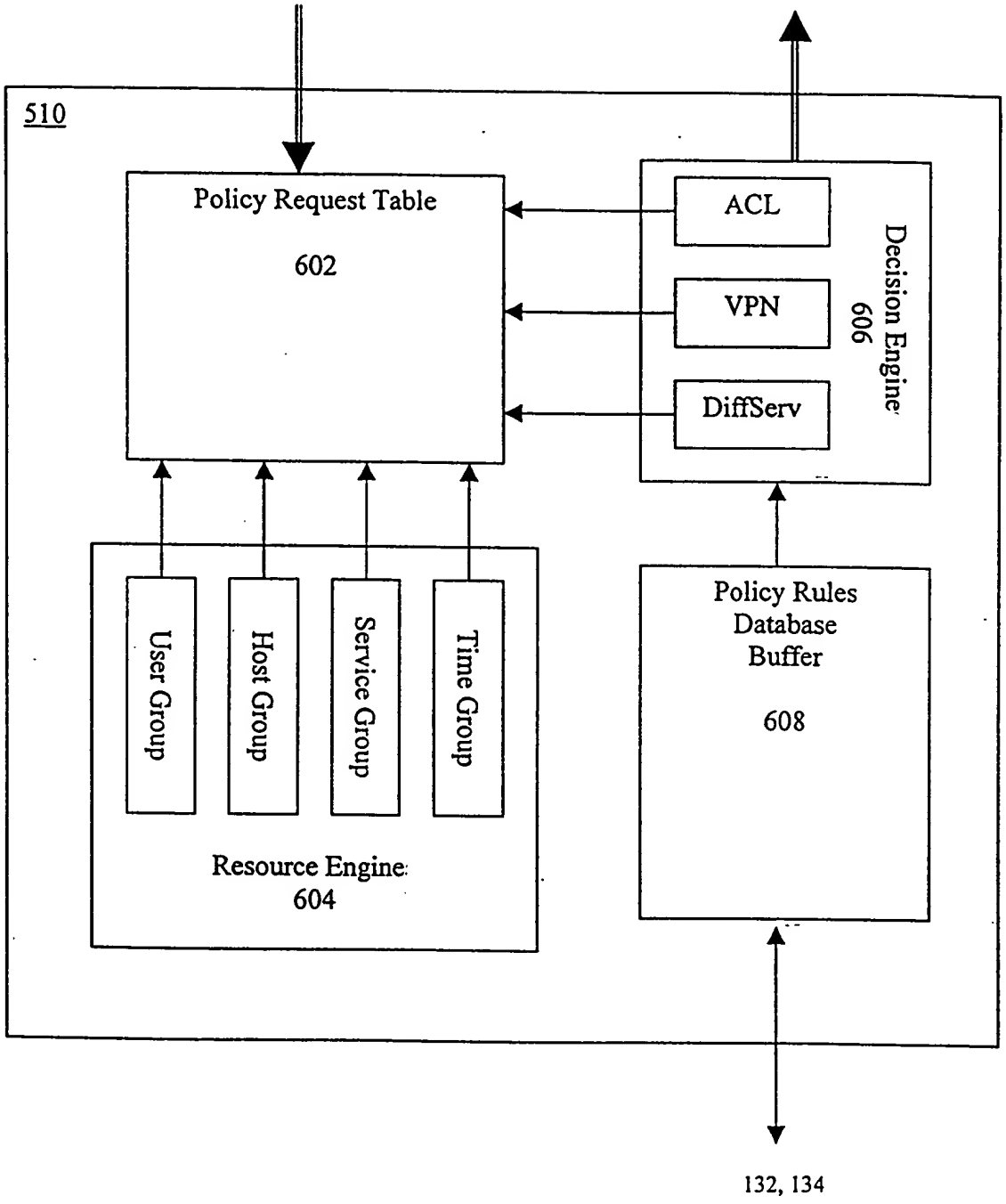

510
Policy Request Table
602
ACL
VPN
DiffServ
Decision Engine
606
User Group
Host Group
Service Group
Time Group
Resource Engine
604
Policy Rules
Database
Buffer
608
132, 134

FIG. 19

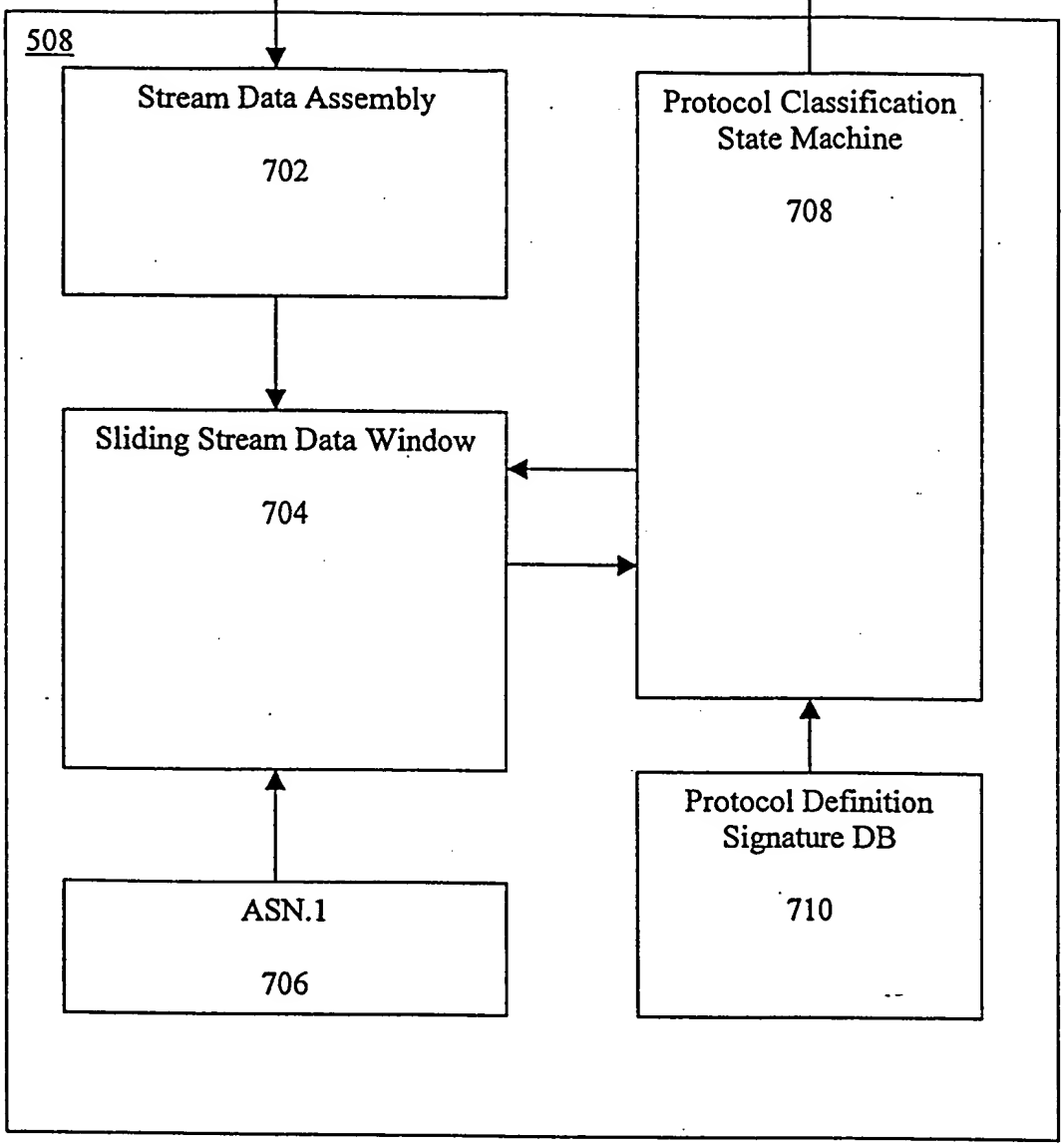

508
Stream Data Assembly
702
Protocol Classification State Machine
708
Sliding Stream Data Window
704
ASN.1
706
Protocol Definition Signature DB
710

FIG. 20

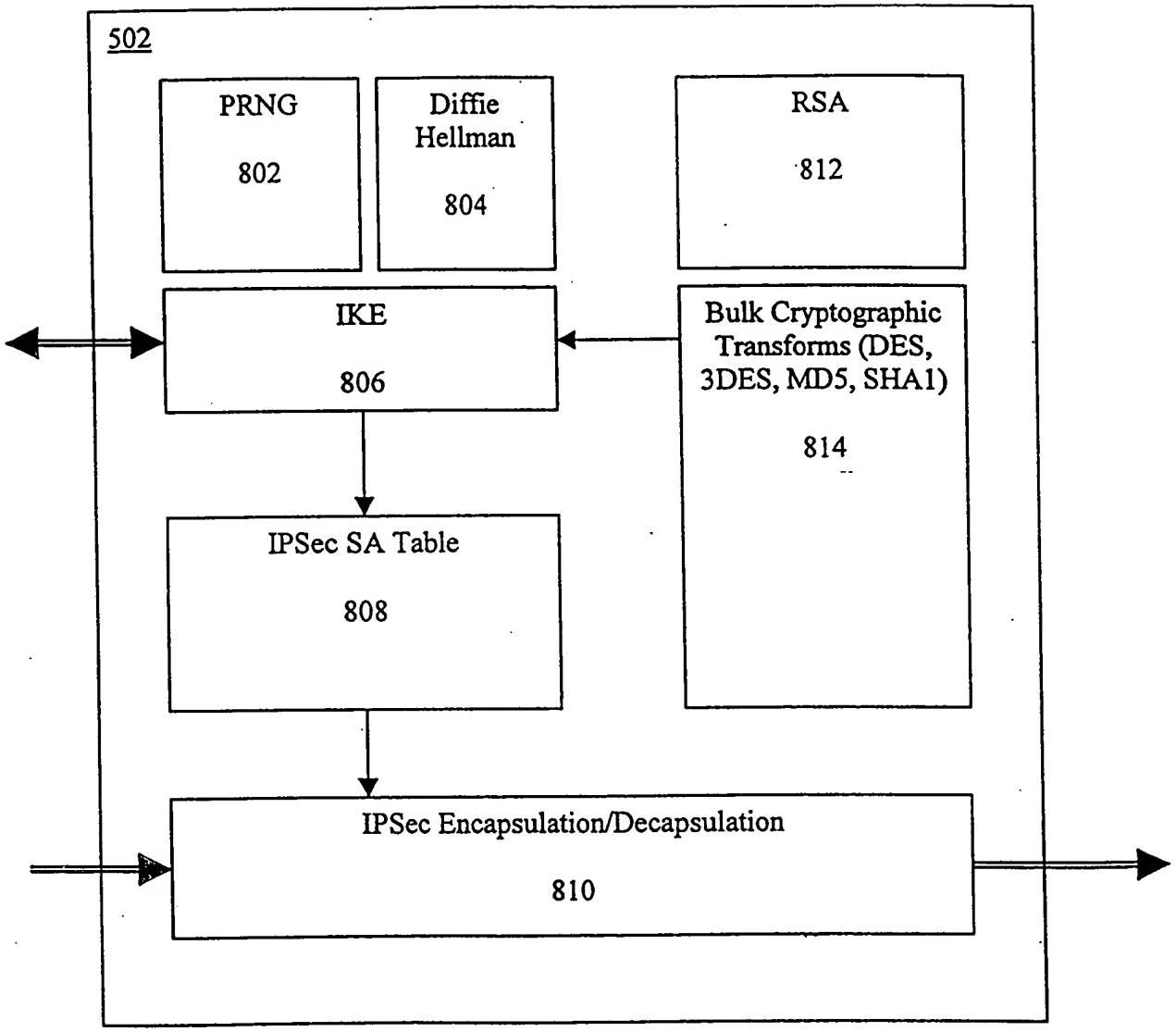

502
PRNG
802
Diffie Hellman
804
RSA
812
IKE
806
Bulk Cryptographic Transforms (DES, 3DES, MD5, SHA1)
814
IPSec SA Table
808
IPSec Encapsulation/Decapsulation
810

FIG. 21

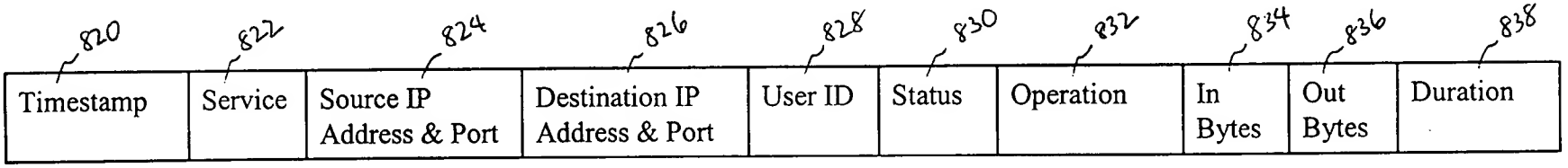

820
822
824
826
828
830
832
834
836
838
Timestamp
Service
Source IP Address & Port
Destination IP Address & Port
User ID
Status
Operation
In Bytes
Out Bytes
Duration

FIG. 22

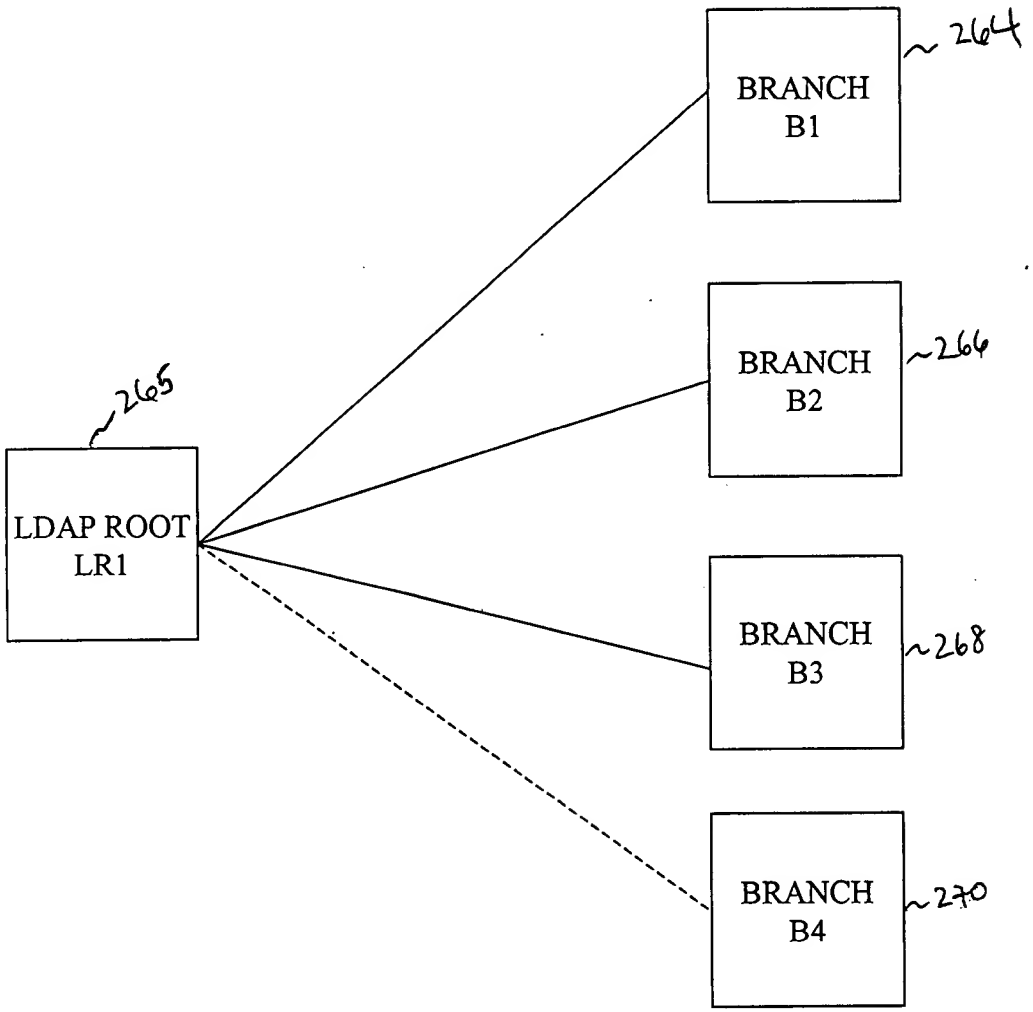

LDAP ROOT
LR1
265
BRANCH
B1
264
BRANCH
B2
266
BRANCH
B3
268
BRANCH
B4
270

FIG. 23

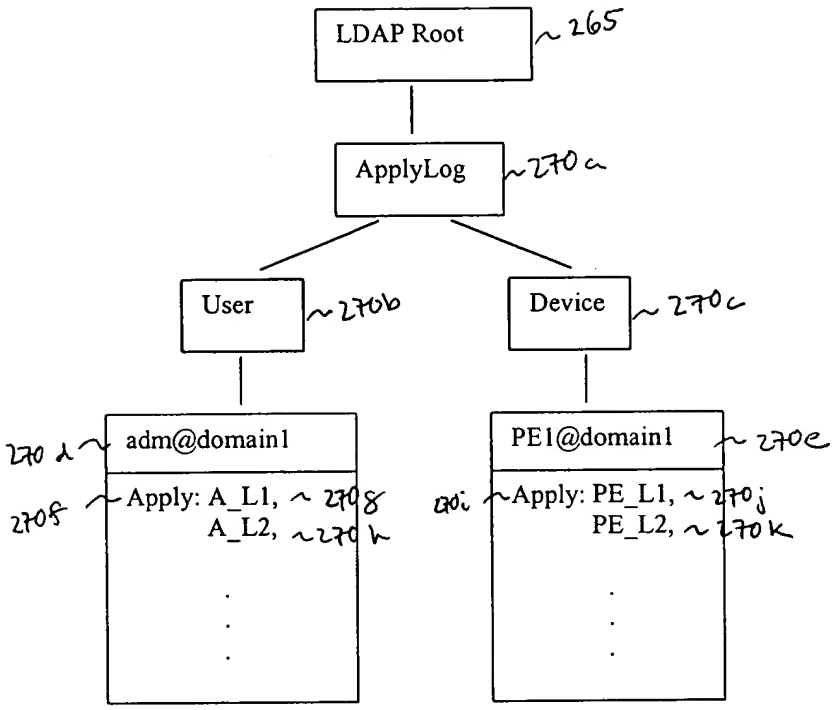
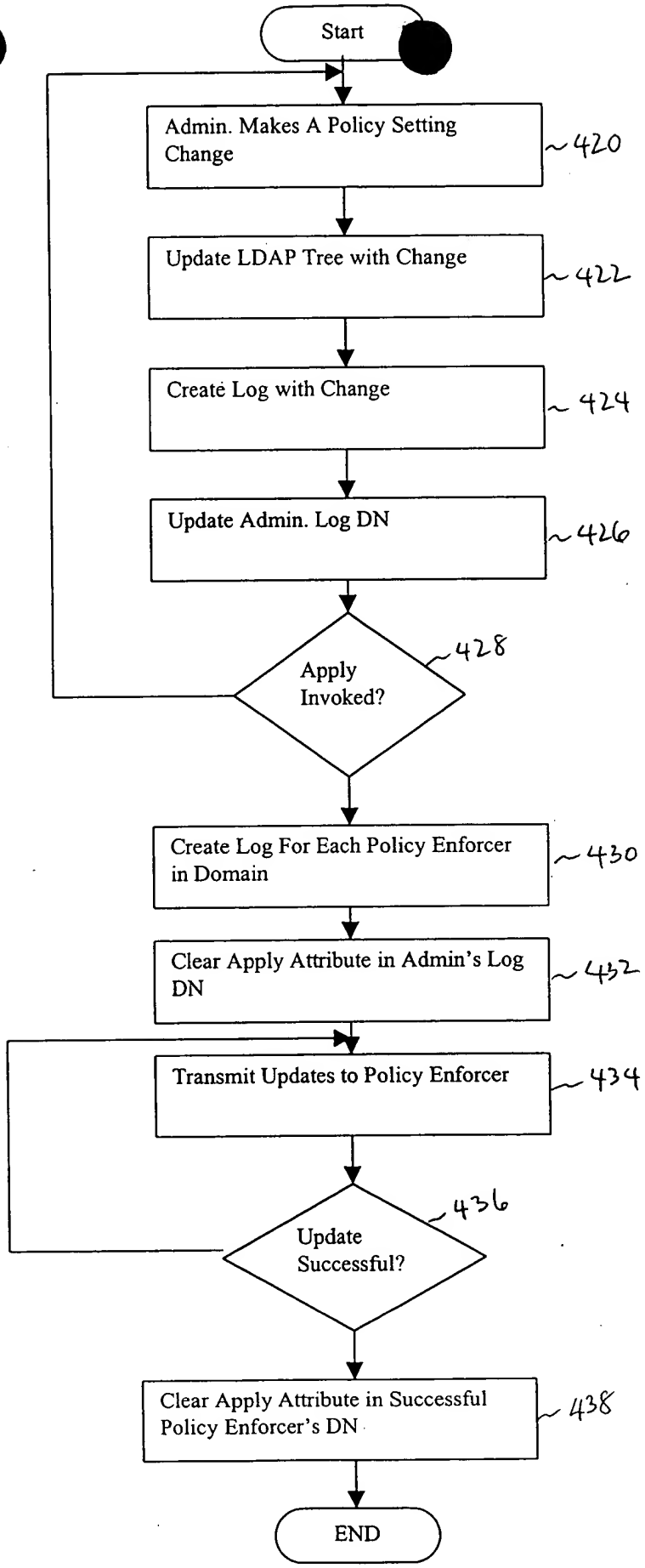

LDAP Root
265
ApplyLog
270a
User
270b
Device
270c
270d
adm@domain1
270e
PE1@domain1
270f
Apply: A_L1, 270g
A_L2, 270h
270i
Apply: PE_L1, 270j
PE_L2, 270k

FIG. 24

FIG. 25


Start
Admin. Makes A Policy Setting Change
420
Update LDAP Tree with Change
422
Create Log with Change
424
Update Admin. Log DN
426
Apply Invoked?
428
Create Log For Each Policy Enforcer in Domain
430
Clear Apply Attribute in Admin's Log DN
432
Transmit Updates to Policy Enforcer
434
Update Successful?
436
Clear Apply Attribute in Successful Policy Enforcer's DN
438
END

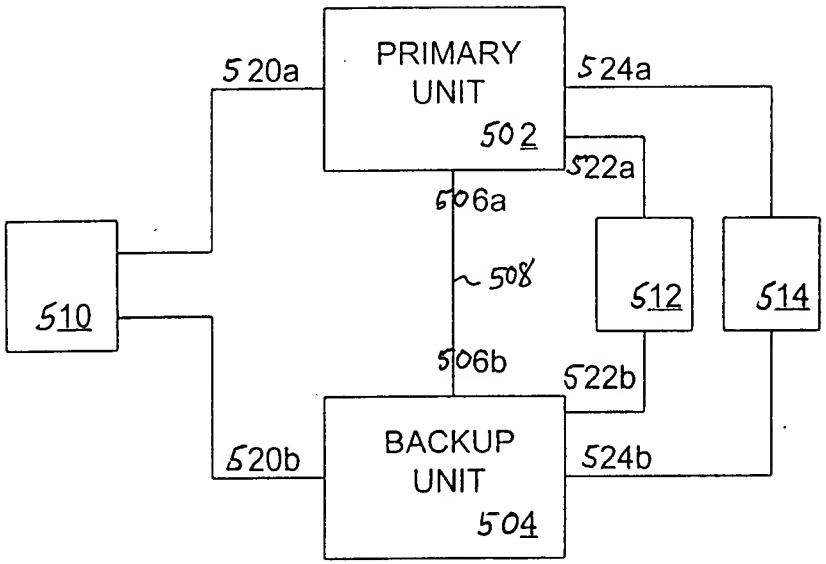

PRIMARY
UNIT
502
520a
524a
522a
506a
508
510
512
514
506b
522b
520b
BACKUP
UNIT
504
524b

Figure 26

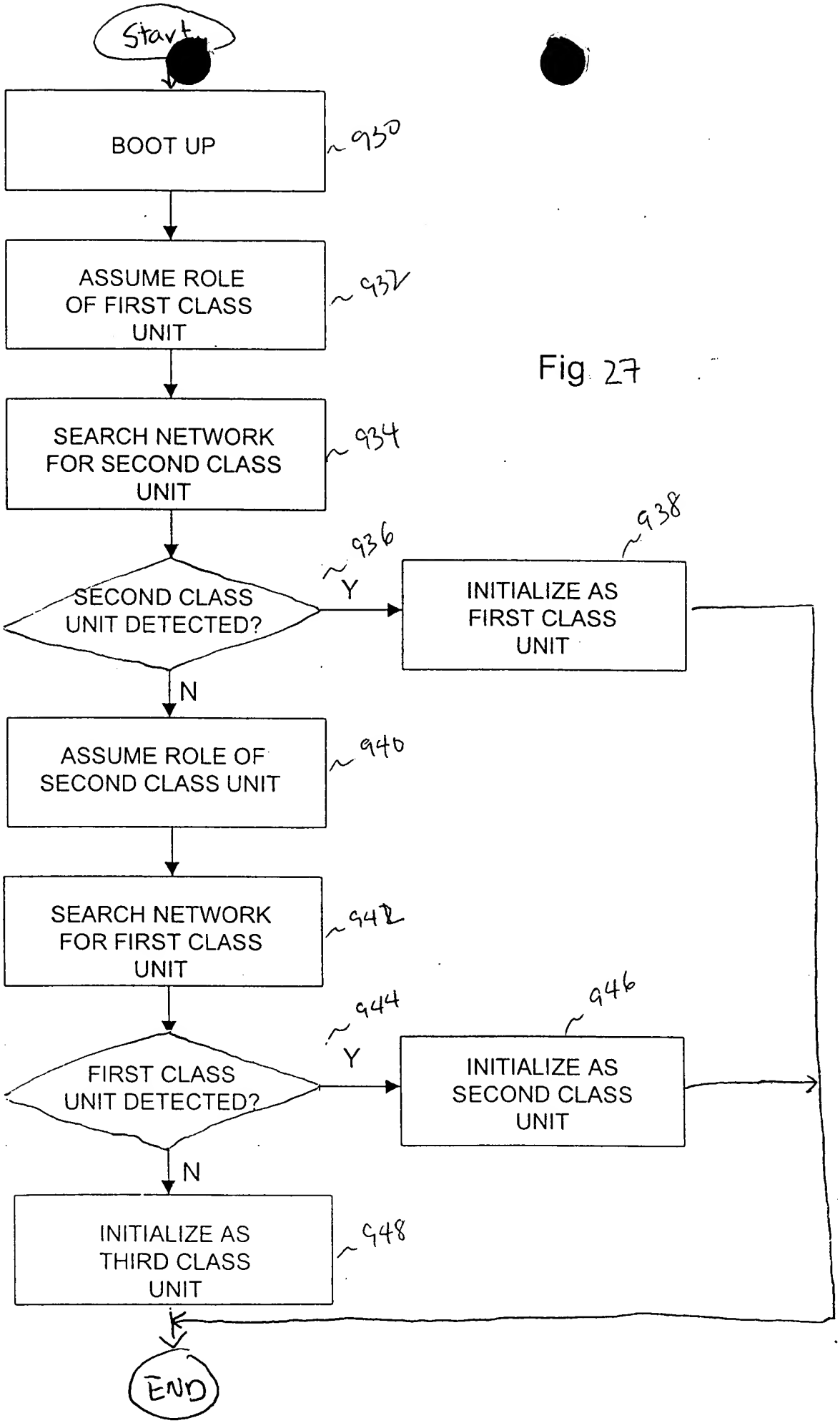

Start
BOOT UP
950
ASSUME ROLE OF FIRST CLASS UNIT
932
SEARCH NETWORK FOR SECOND CLASS UNIT
934
SECOND CLASS UNIT DETECTED?
936
Y
938
INITIALIZE AS FIRST CLASS UNIT
N
ASSUME ROLE OF SECOND CLASS UNIT
940
SEARCH NETWORK FOR FIRST CLASS UNIT
942
FIRST CLASS UNIT DETECTED?
944
Y
946
INITIALIZE AS SECOND CLASS UNIT
N
INITIALIZE AS THIRD CLASS UNIT
948
END

Fig. 27

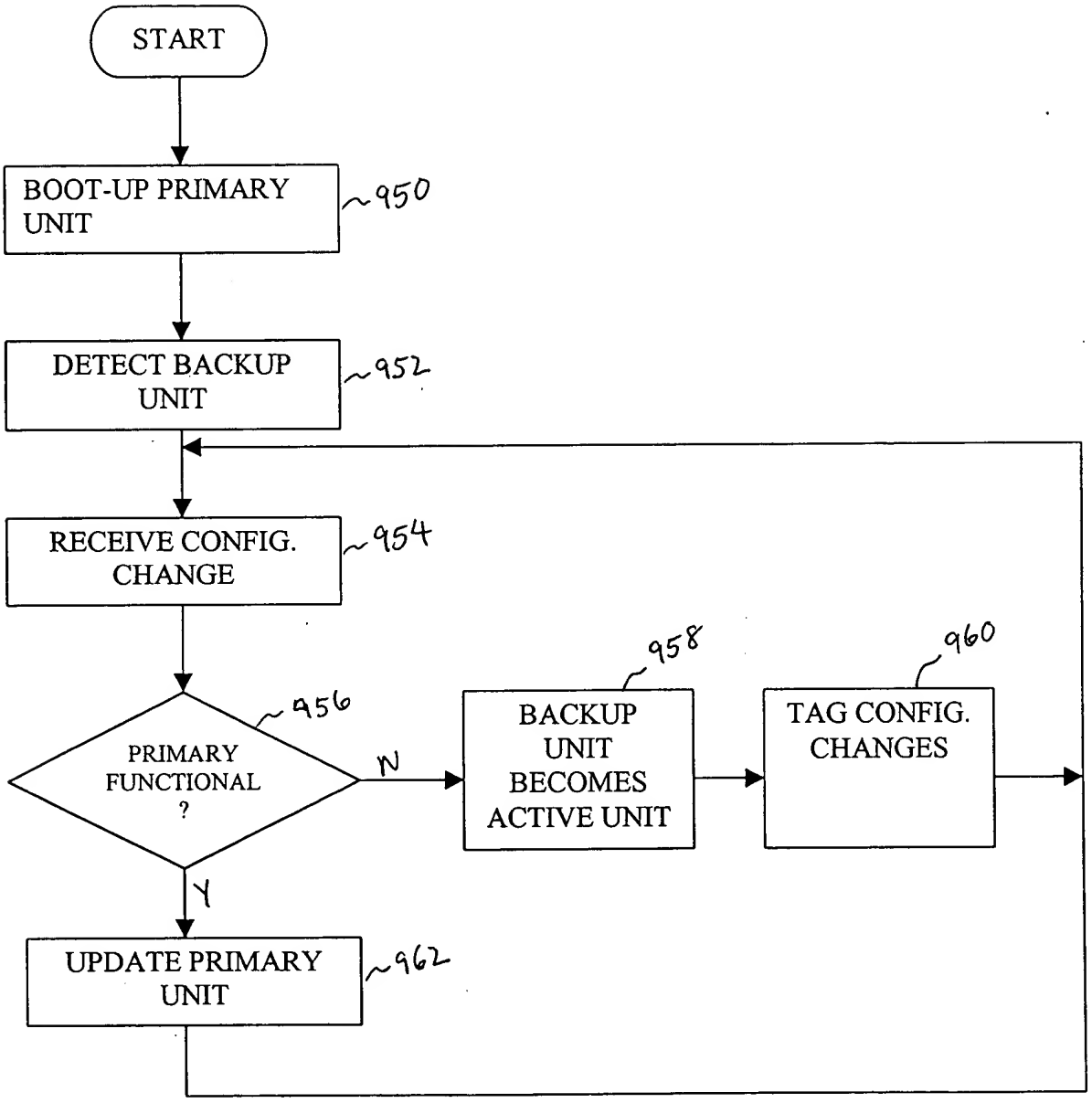

START
BOOT-UP PRIMARY UNIT
950
DETECT BACKUP UNIT
952
RECEIVE CONFIG. CHANGE
954
PRIMARY FUNCTIONAL ?
956
N
Y
BACKUP UNIT BECOMES ACTIVE UNIT
958
TAG CONFIG. CHANGES
960
UPDATE PRIMARY UNIT
962

FIG. 28

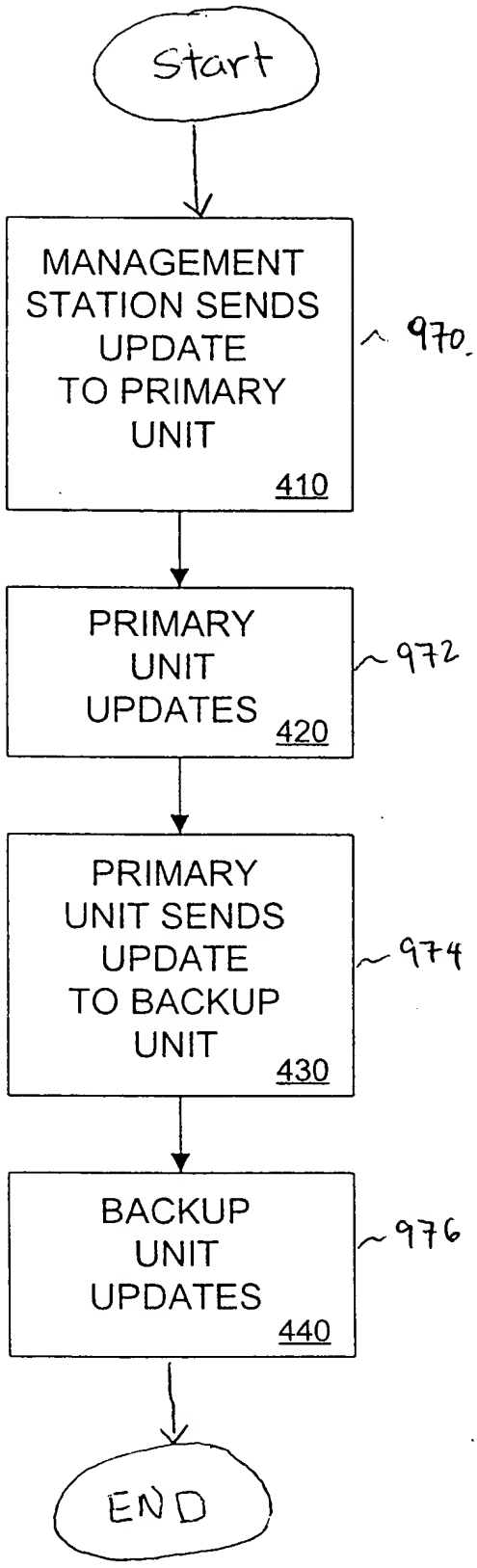

Start
MANAGEMENT STATION SENDS UPDATE TO PRIMARY UNIT
410
970
PRIMARY UNIT UPDATES
420
972
PRIMARY UNIT SENDS UPDATE TO BACKUP UNIT
430
974
BACKUP UNIT UPDATES
440
976
END

Fig 29

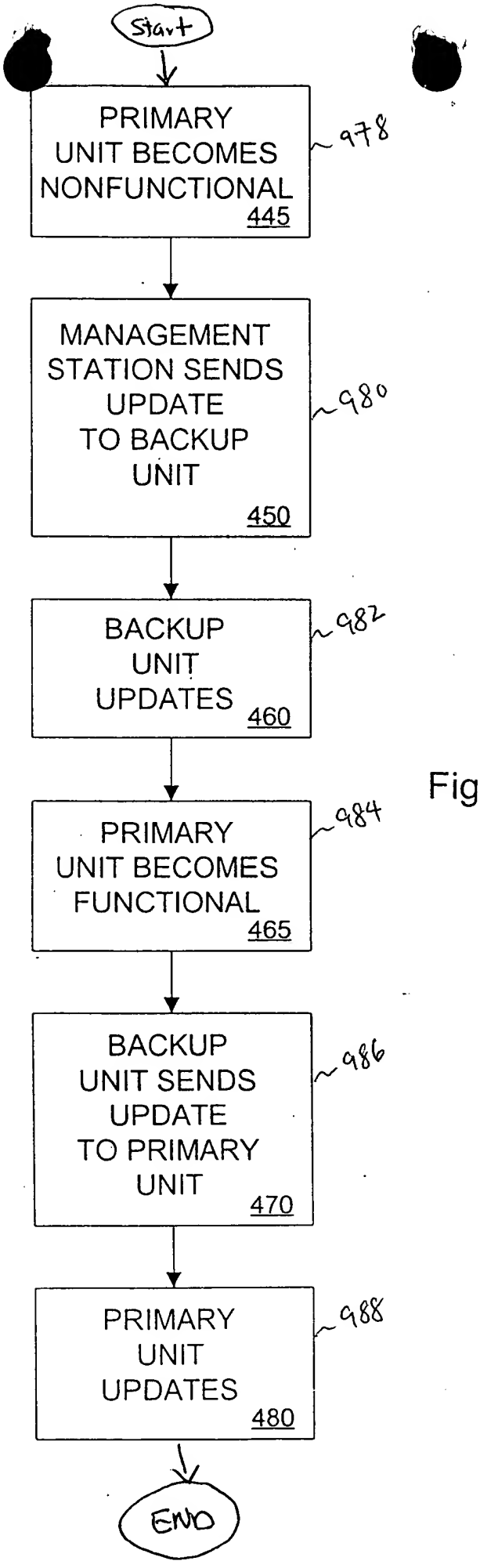

Start
PRIMARY UNIT BECOMES NONFUNCTIONAL 445
978
MANAGEMENT STATION SENDS UPDATE TO BACKUP UNIT 450
980
BACKUP UNIT UPDATES 460
982
PRIMARY UNIT BECOMES FUNCTIONAL 465
984
BACKUP UNIT SENDS UPDATE TO PRIMARY UNIT 470
986
PRIMARY UNIT UPDATES 480
988
END

Fig. 30